UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,057	08/30/2001	Gregor P. Freund	VIV/0003.01	8336

28653 7590 11/28/2005

JOHN A. SMART
708 BLOSSOM HILL RD., #201
LOS GATOS, CA 95032

EXAMINER	
DIVECHA, KAMAL B	
ART UNIT	**PAPER NUMBER**
2151	

DATE MAILED: 11/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/944,057
Filing Date: August 30, 2001
Appellant(s): FREUND ET AL.

John A. Smart
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed September 12, 2005 appealing from the Office action mailed April 7, 2005.

(1) Real Party in Interest

The appellant's statement of the real party in interest contained in the brief is correct.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,463,474	Fuh	10-2002
5,761,683	Logan	06-1998
6,026,440	Shrader	02-2000
6,542,933	Durst	04-2003

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

1. Claims 1, 3-6, 8-9, 11-12, 17, 21, 45-51, 55 and 57 are rejected under 35 U.S.C. 102(e) as being anticipated by Fuh et al (hereinafter Fuh, U.S. Patent No. 6,463,474 B1).

As per claim 1, Fuh discloses a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers (figure 3 item #306, item #210, item #216 and fig. 1 item #124, 128), a method for managing Internet access based on a specified access policy (see abstract; col. 3 L40 to col. 4 L13, the authentication and authorization process by Fuh is considered the process of managing internet access based on the policy), the method comprising: transmitting a challenge from said client premises equipment to each client computer (applicant fails to define the term "challenge", therefore examiner simply interpreted the term as a login web page presented or transmitted by the firewall router to the client, fig. 4 item #403), for determining whether a given client computer is in compliance with said specified access policy (please note applicant fails to define the access policy in the claim, therefore examiner simply interpreted access policy as a policy that governs the access to a resource); transmitting a response from at least one client computer

back to said client premises equipment, for responding to said challenge that has been issued (i.e. user provides the username and password as the reply to the login web page, fig. 4 item #404); and blocking Internet access for any client computer that does not respond appropriately to said challenge (i.e. if the authentication and authorization fails, client would be blocked from accessing the target server, fig. 7A block #707; fig. 7B item #738; col. 1 L58 to col. 2 L7; col. 7 L40-46).

As per claim 3, Fuh discloses the process wherein a client computer that responds with a particular predefined code indicating non-compliance is blocked from Internet access (figure 7B step #726, #728, #730 and #738).

As per claim 4, Fuh discloses the process wherein a client computer that responds with a particular predefined code indicating compliance is permitted Internet access (figure 7A step #702, #704, #706 and #712).

As per claim 5, Fuh discloses the process wherein before receipt of a challenge, transmitting an initial message from a particular client computer to the client premises equipment (figure 4 item #401 sent before #403), for requesting the client premises equipment to transmit a challenge to that particular client computer.

As per claim 6, Fuh discloses the process wherein said initial message comprises a client hello packet (read as a data or http packet or request: figure 4 item #401).

As per claim 8, Fuh discloses the process wherein said access policy specifies rules that govern Internet access by the client computers (column 5 line 67 to column 6 lines 1-5 and col. 14 L20-30).

As per claim 9, Fuh inherently teaches the process of blocking Internet access including determining whether permitting Internet access for a given client computer would violate any of said rules, and if permitting such Internet access would violate any of said rules, denying Internet access for that client computer (fig. 7A and fig. 7B).

As per claim 11, Fuh discloses the process wherein said access policy specifies which applications (read as types of network traffic) are allowed Internet access (column 7 lines 56-58 and col. 13 L44 to col. 14 L30: table 2 provides an example of applications such as ftp, telnet, smtp that are allowed access).

As per claim 12, Fuh discloses the process wherein said access policy (interpret as policies defined by authorization and authentication process) specifies applications (read as types of network traffic) that are allowed Internet access (column 7 lines 56-58).

As per claim 17, Fuh discloses the process wherein said access policy specifies Internet access activities that are permitted or restricted for applications or versions thereof (column 7 lines 56-60; column 5 lines 58-67 to column 6 lines 1-5 and col. 13 L44 to col. 14 L30).

As per claim 21, Fuh discloses the process wherein said challenge includes a request (read as login request) for a particular client computer to respond as to whether it is in compliance with said access policy (figure 4 login request 403 and response 404).

As per claim 45, Fuh discloses a system for regulating Internet access by client computers (see abstract) comprising: an access policy (read as access privileges) governing Internet access by said client computers (column 6 lines 1-5); client premises equipment serving a routing function (figure 3 item #210) for each client computer to be regulated and capable of issuing a challenge to each client computer (figure 4 a login arrow showed by 403), for

determining whether a given client computer is in compliance with said access policy; one or more client computers which can connect to the Internet (column 3 lines 30-35) and at least one of which can respond to challenges issued by said client premises equipment (figure 4 login 403 and response 404); and an enforcement module for selectively blocking Internet access to the Internet to client computers not in compliance with said access policy (figure 4 block #400 and column 11 lines 30-33).

As per claim 46, Fuh discloses the system wherein said client premises equipment includes a router (figure 3 block #210; fig. 2 item #210).

As per claim 47, Fuh discloses the system wherein said access policy is provided at each client computer to be regulated (figure 5A item #504 and 506 which are part of access policy for authentication).

As per claim 48, Fuh discloses the system wherein said enforcement module is provided at said client premises equipment (figure 4 block #400 in block #210).

As per claim 49, Fuh discloses the system wherein said at least one client computer capable of responding to challenges can respond (figure 4 item #404) with a particular predefined code indicating non-compliance (incorrect username and password) with said access policy is blocked from Internet access (figure 7B step #726, #728, #730 and #738).

As per claim 50, Fuh discloses the system wherein a client computer that responds with a particular predefined code (figure 4 item #404) indicating compliance (correct username and password) with said access policy is permitted Internet access (figure 7A step #702, #704, #706 and #712).

As per claim 57, Fuh discloses the system wherein said access policy specifies types of activities which applications are allowed to perform or restricted from performing (column 7 lines 55-58).

As per claims 51 and 55, they do not teach or further define over the limitations in claims 1, 3-6, 8-9, 11-12, 17, 21, 45-50 and 57. Therefore the claims 51 and 55 are rejected for the same reasons as set forth in claims 1, 3-6, 8-9, 11-12, 17, 21, 45-50 and 57.

2. Claims 2, 7, 10, 13-16, 18-20, 52-54, 56, 58-60 are rejected under 35 U.S.C. 103(a) as being obvious over Fuh et al (U.S. Patent No. 6,463,474 B1).

As per claim 2, Fuh does not explicitly show a client computer that does not respond at all is blocked from the Internet access, however Fuh does provide a login page (figure 5A) to client (read as a challenge), wherein if a client does not respond or provide the login information, than the client would be blocked from accessing the network resources, therefore it would have been obvious to the one of ordinary skilled in the art at the time the invention was made to block a client from accessing the network resources that does not respond at all to the login because this would have created a secure communication system in a network preventing the resources from hackers and intruders.

As per claim 7, Fuh does not explicitly show that the client premises equipment is capable of permitting Internet access by selected client computers and denying access to the other client computers, but Fuh et al does shows plurality of users connected to the router (figure 2 item #208a, b and c and item #210) and routers performing the authentication functions wherein if a client fails to provide correct information to the router then a router would block the

traffic (figure 7A block #707) to that particular client and when the client provides the correct information, it would be allowed to access the resources or the target server(figure 7A block #712). Therefore based on the Fuh's teaching, Fuh's system is capable of permitting internet access by selected client computers and denying access to the other client computers.

As per claim 10, Fuh does not explicitly show that the access policy includes rules that are enforced against selected ones of users, computers, and groups thereof, But Fuh does teach the access policy including rules that are enforced against users accessing the target server (col. 7 L16-61). Therefore it would have been obvious to the one of ordinary skilled in the art to enforce the rules in the access policy against selected ones of users, computers and groups in order to avoid any unnecessary incoming or outgoing traffic to the network.

As per claims 13-16, Fuh discloses the process of hashing information such as source IP address, destination IP address, source port, destination port value and state information (col. 9 L55-63), however Fuh does not disclose the applications are specified by executable name and version number, application are specified by digital signatures, digital signatures are computed using a cryptographic hash and wherein said cryptographic hash comprises a selected one of Secure Hash Algorithm (SHA-1) and MD5 cryptographic hashes, however it would have been obvious to the one of ordinary skill in the art at the time the invention was made to incorporate these features because they are simply well known and obvious in the art and modify Fuh in order to specify the applications by their executable name and version numbers, specify applications by the digital signatures, wherein digital signatures are computed using cryptographic hash and wherein cryptographic hash comprises secure hash algorithm and MD5 cryptographic hashes. One of ordinary skilled in the art would have been motivated because it

would have allowed a router to make a correct decision (block or permit) by comparing executable names and securely transfer the data to the destination by searching the profile efficiently.

As per claims 18 and 19, Fuh does not explicitly disclose access policy with rules are transmitted to client computers from a remote location and remote location comprising a centralized location for maintaining said access policy but Fuh does show a centralized location where access policy (authentication information and access privileges of users) would have been maintained (figure 3 block #218 and 220 and col. 13 L60-65) and the link between the client and the centralized location from where the data would have been transferred (figure 3: the communication link 310).

As per claim 20, Fuh discloses the process of authenticating user based on username and password and applying the user profile to the user (col. 7 L47 to col. 8 L6), however Fuh does not teach the process of determining, based on identification of a particular client computer or group thereof, a specific subset of rules filtered for that particular client computer or group thereof. But it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Fuh in order to determine based on identification of a client a specific subset of rules filtered for that particular client because user profiles (as in Fuh) are implemented for specific users and applied to that particular user only because it would have validated the user (Fuh, col. 8 L4-6).

As per claims 52-54, 56 and 58-60, they do not teach or further define over the limitations in claims 2, 7, 10, 13-16 and 18-20. Therefore claims 52-54, 56 and 58-60 are rejected for the same reasons as set forth in claims 2, 7, 10, 13-16 and 18-20.

3. Claims 22-25, 27-40 and 42-44 are rejected under 35 U.S.C. 103(a) as being obvious over Fuh et al (U.S. Patent No. 6,463,474 B1) in view of Logan et al (U.S. Patent No. 5,761,683).

As per claim 22, Fuh discloses the process of informing a client computer that is not in compliance with access policy (fig. 7B item #736), however Fuh does not teach the process of redirecting a client computer that is not in compliance with said access policy to a sandbox server. Logan teaches the process of redirecting a request (i.e. a client computer) to a locally-stored resources (i.e. locally stored resources available at local server, col. 19 L60-67; col. 20 L24-37). Therefore it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Fuh in view of Logan in order to redirect a client computer that is not in compliance with access policy to a sandbox server (read as a server), since Logan teaches the process of redirecting a client computer to another server. One of ordinary skilled in the art would have been motivated so that the client computer can retrieve the locally stored copies of the document from a local server (Logan, col. 10 L63-67).

As per claim 23, Fuh in view of Logan discloses the process of redirecting a client computer that is not in compliance with a particular access policy to a particular port on the sandbox server (please note, the check for the compliance is disclosed by Fuh and the process of redirecting is disclosed by Logan, and it is obvious that the client computer would be directed to a particular port on the server, see claim 22); and Logan further discloses the process of displaying particular error message pages on the server in response to communications on particular ports (column 7 lines 41-48). Therefore it would have been obvious to further modify Fuh in view of Logan, in order to display error messages on the server in response to

communications, since Logan teaches the process of displaying error messages on the server. One of ordinary skilled in the art would have been motivated because it would have indicated to the user of the computer that the access did not succeed (Logan, col. 7 L45-50).

As per claim 24, Fuh discloses a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers (figure 3 item #306, item #210, item #216 and fig. 1 item #124, 128), a method for managing Internet access based on a specified access policy (see abstract; col. 3 L40 to col. 4 L13, the authentication and authorization process by Fuh is considered the process of managing internet access based on the policy), the method comprising: transmitting a challenge from said client premises equipment to each client computer (applicant fails to define the term "challenge", therefore examiner simply interpreted the term as a login web page presented or transmitted by the firewall router to the client, fig. 4 item #403), for determining whether a given client computer is in compliance with said specified access policy (please note applicant fails to define the access policy in the claim, therefore examiner simply interpreted access policy as a policy that governs the access to a resource); transmitting a response from at least one client computer back to said client premises equipment, for responding to said challenge that has been issued (i.e. user provides the username and password as the reply to the login web page, fig. 4 item #404), however, Fuh does not explicitly disclose the process of redirecting a request for Internet access by any client computer that does not respond appropriately to said challenge to a sandbox server. Logan discloses the process of redirecting a request (i.e. a client computer) to a locally-stored resources (i.e. locally stored resources available at local server, col. 19 L60-67; col. 20 L24-37). Therefore it would have been obvious to a person of ordinary skilled in the art at the time the

invention was made to modify Fuh in view of Logan in order to redirect a client computer that is not in compliance with access policy to a sandbox server (read as a server), since Logan teaches the process of redirecting a client computer to another server. One of ordinary skilled in the art would have been motivated so that the client computer can retrieve the locally stored copies of the document and/or web page from a local server according to Logan (Logan, col. 10 L63-67).

As per claims 25, 27, 31 and 40, they do not teach or further define over the limitations in claims 22-24. Therefore claims 25, 27, 31 and 40 are rejected for the same reasons as set forth in claims 22-24.

As per claims 28-30, 32-39 and 42-44, they recite similar limitations as in claims 4-6, 10-11, 13, 17-21 and 42-44. Therefore claims 28-30, 32-39 and 42-44 are rejected for the same reasons as set forth in claims 4-6, 10-11, 13, 17-21 and 42-44 (see above).

4. Claims 26 and 41 are rejected under 35 U.S.C 103(a) as being obvious over Fuh et al (U.S. Patent No. 6,463,474 B1) in view of Logan et al (U.S. Patent No. 5,761,683) in further view of Shrader et al (U.S. Patent No. 6,026,440).

As per claim 41, Fuh discloses the process of blocking computers that are not in compliance with other access policies from accessing the Internet (fig. 7A block #707; fig. 7B item #738; col. 1 L58 to col. 2 L7; col. 7 L40-46), however, Fuh does not disclose the process of permitting client computers that are not in compliance with particular access policies to elect to access the internet.

Shrader explicitly discloses a web server account manager plug-in for monitoring resources. Shrader further teaches a server returning an error message (e.g. Unauthorized) to the

browser (i.e. to the computer or client) and prompting the user (client) for id and password (i.e. providing the user with another opportunity to elect to access the internet again by submitting login and password again, column 4 lines 56-67).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to incorporate the teaching of Shrader as stated above with the Fuh and Logan in order to permit clients that are no in compliance with particular access policies to elect to access internet. One of ordinary skilled in the art would have been motivated because it would have avoided the network congestion at the router and improved routers performance and would have improved the system efficiency by allowing clients to elect to access the Internet one more time.

As per claim 26, it does not teach or further define over the limitations in claim 41. Therefore claim 26 is rejected for the same reasons as set forth in claim 41.

5. Claim 61 is rejected under 35 U.S.C 103 (a) as being obvious over Fuh et al (U.S. Patent No. 6,463,474 B1) in view of Durst, Jr. et al (U.S. Patent No. 6,542,933 B1).

As per claim 61, Fuh discloses a system comprising a target server, firewall router and one or more clients (fig. 1-2) and the process for determining whether the client is in compliance to access the network (fig. 7B), however Fuh does not disclose a sandbox server to which client computers that are not in compliance with said access policy are redirected.

Durst, explicitly disclose a system and method of using machine-readable or human-readable linkage codes for accessing networked data resources. He further teaches redirecting a client computer from an information server to a content server (read as sandbox server, column 3 lines 19-21 and lines 65-67 and figure 2 block #60). Therefore it would have been obvious to a

person of ordinary skilled in the art at the time the invention was made to modify Fuh in view of Durst, in order to include a sandbox server to which the client computers that are not in compliance are redirected, since Durst teaches the process of redirecting the client to another server.

One of ordinary skilled in the art would have been motivated because it would have improved the routers performance by redirecting the unauthorized traffic to another server and would have also avoided network congestion at the router.

6. Claims 62-64 are rejected under 35 U.S.C 103 (a) as being obvious over Fuh et al (U.S. Patent No. 6,463,474 B1) in view of Durst, Jr. et al (U.S. Patent No. 6,542,933 B1) and in further view of Shrader et al (U.S. Patent No. 6,026,440).

As per claim 62, Fuh in view of Durst does not disclose the process of wherein the sandbox server informs non-compliant client computers that they are not in compliance with said access policy. Shrader explicitly discloses a web server account manager plug-in for monitoring resources. Shrader further teaches the process wherein the clients are notified (read as inform) by returning error message such as unauthorized (i.e. not in compliance) to the browser (column 4 lines 56-67 and figure 3). Therefore it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Fuh in view of Durst, further in view of Shrader, in order to inform the clients of the non-compliance. One of ordinary skilled in the art would have been motivated because it would have informed the client of the unauthorized access (Shrader, col. 4 L64-66).

As per claim 63, Shrader further discloses the process wherein the client computers are allowed to elect to access the Internet (prompting a user for user id and password) after being informed that they are unauthorized (return error message) or they are not in compliance with access policy (column 4 lines 56-67).

As per claim 64, Durst discloses the information server (read as enforcement module) redirecting the client computers to the content server to retrieve primary content file (column 3 lines 19-21) and Shrader et al teaches a server capable of displaying error messages (column 4 lines 56-66).

(10) Response to Argument

The examiner summarizes the appellant's arguments presented in the appeal brief and addresses each argument individually.

As per appellant's arguments filed on September 12, 2005, the appellant argues in substance that:

a. The examiner failed to establish anticipation of claimed invention under section 102 because Fuh fails to teach each and every element set forth in claims 1 and 45 (see page 7). More specifically, appellant argues the following:

i. Fuh does not describe an access policy for managing Internet (page 8).

Appellant argues that Fuh's system decides whether to authenticate a user for access to particular resource based on user login information, while appellant's security system serves a different purpose in enforcing compliance by client computers. In Appellant's system, "the

access policy may specify which particular applications are allowed Internet access", thereby allowing users (including administrators) to block spyware and other malware from accessing the Internet from a given client machine (page 7).

However, appellant's claim 1 and 45 fails to explicitly teach, suggest and disclose the specified access policy that would specify which particular applications are allowed access to the Internet.

Independent claims 1 and 45 simply states:

"A system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers, a method for managing Internet access based on a **specified access policy,** the method comprising:

transmitting a challenge from said client premises equipment to each client computer, for determining whether a given client computer is in compliance with said **specified access policy**;

transmitting a response from at least one client computer back to said client premises equipment, for responding to said challenge that has been issued; and

blocking Internet access for any client computer that does not respond appropriately to said challenge".

Nowhere in the claim is it stated that the "specified access policies" may specify which applications are allowed access to the Internet. Therefore the specified access policy is interpreted to be any policy that would govern the access to the network or Internet based on the broadest reasonable interpretation.

The process of authentication and authorization disclosed by Fuh is the process of managing Internet access based on specified access policy because if the user does not supply correct username and password, the user is considered a non-compliant and therefore would not be granted access, and if the user is authenticated with the correct username and password, authorization is performed which determines which applications are allowed access to the Internet and/or target server.

In Fuh's system the process of managing Internet access and/or access to the target server based on the specified access policy comprises two phases, first phase is authentication and second phase is authorization. Authentication validates the client and/or user by requesting from the client authentication information such as username and password. After the client is authenticated the firewall performs authorization process. In the authorization process, the user profile is consulted to determine which types of applications are allowed access to the target server and/or Internet (col. 2 L32-54: the user profile specifies specific type of traffic that are allowed to pass the firewall router, e.g. ftp traffic wherein ftp is an application; (Fuh, col. 7 L47-60 and col. 13 L60 to col. 14 L30).

ii. Appellant's access policy relates to Internet access by client computers and not to a particular resource (page 8).

In reply to [a. (ii)]: Fuh's authentication proxy is implemented at a firewall router which protects a particular network resource at target server from access by external users **as well as** access to the Internet by the users of the clients from within the intranet (col. 7 L27-46). Fuh further teaches the use of Access Control Lists, which regulates the inbound, and outbound network traffic (i.e. traffic coming into the intranet and traffic going out to Internet, col. 9 L30-55; col. 14 L20-30: provides the examples of the applications such as telnet, ftp, smtp, that are allowed access associated with the user profile). Fuh's system is not limited to authenticate the user for access to the network resource, but it is also directed to manage the Internet access from within the intranet based on the access policy. Fuh explicitly states "a user of a client from within the intranet attempts to access a target server or other resource that is not part of the same

intranet as that of the client" (col. 7 L27-30); and "the http packets are intercepted by a firewall that protects the intranet from unwanted traffic originating from the Internet (inbound traffic) and **can prevent users of clients from within intranet from accessing undesirable web sites on the Internet** (outbound traffic)" (col. 7 L40-45), as the LAN and intranet are both connected to a global network such as Internet (col. 8 L12-13).

Therefore Fuh does describe an access policy for managing Internet access by client computers (authentication and authorization is fully described at col. 10 L5 to col. 12 L56).

The firewall router of Fuh controls both the remote access to Intranet (inbound traffic) as well as accessing the Internet (outbound traffic) as discussed above.

iii. Fuh's access privileges are not comparable to appellant's claim element of Internet access based on a specified access policy (page 9).

In reply to [a. (iii)]: Fuh's access privileges are comparable to appellant's claim element of "managing Internet access based on a specified access policy" which governs Internet access by the client computers because appellant failed to distinctly claim the subject matter in claims 1 and 45 as discussed above.

Appellant argues that the challenge issued by Fuh's system requests login information for authenticating a user (i.e. examines the compliance by comparing the username and password, considered as access policy, if the username and password is correct, grant access and if not deny access), whereas appellant's invention, in contrast, issues a challenge to a client computer for determining whether the client computer is in compliance with the above-described access policy (i.e. as cited on page 7) governing Internet access by client computers (page 9), however

appellant failed to distinctly incorporate or suggest the subject matter (i.e. above-described access policy which may specify which particular applications are allowed Internet access) into the rejected claims 1 and 45.

iv. Unlike Fuh's system, appellant's system does not permit or block requests for access based on user login information. Instead, Appellant's system determines whether a given client computer is in compliance with the specified access policy governing Internet access (page 9-10).

In reply to [a. (iv)]: that Unlike Fuh's system, appellant's invention does not permit or block requests for access based on user login information. Instead, appellant's system determines whether a given client computer is in compliance with the specified access policy governing Internet access, **the claims also does not state, suggest or teach that permitting** or blocking requests for access **is not based on user login information**, it simply suggests that the system determines whether client computer is in compliance with the **specified access policy** (in Fuh's case the specified access policy is specified in the user profile).

v. Another difference between the appellant's system and that of Fuh is that appellant's system provides for blocking access by the client computer to the Internet, while Fuh's system focuses on blocking access by the client computer to a particular resource (intranet, see page 10).

In reply to [a. (v)]: that another difference between appellant's approach and that of Fuh is that appellant's system provides for blocking access by the client computer to the Internet,

while Fuh's system focuses on blocking external access to particular resource, Examiner disagrees. Fuh's system is not limited to blocking external access to particular resource.

But, it is also directed to manage the Internet access from within the intranet. Fuh explicitly states "a user of a client from within the intranet attempts to access a target server or other resource that is not part of the same intranet as that of the client" (col. 7 L27-30); and "the http packets are intercepted by a firewall that protects the intranet from unwanted traffic originating from the Internet (inbound traffic) and **can prevent users of clients from within intranet from accessing undesirable web sites on the Internet** (outbound traffic)" (col. 7 L40-45), as the LAN and intranet are both connected to a global network such as Internet (col. 8 L12-13).

A firewall router disclosed by Fuh is a security system (a client premises equipment serving a routing function for the client computers that are being regulated) that functions and controls both incoming traffic into the intranet and outgoing traffic out of intranet to the Internet (fig. 1; fig. 2 item #210; col. 7 L15-46; col. 1 L60 to col. 2 L7: explicitly teaches that the firewall manages both the incoming and outgoing traffic onto the Internet). As such, Fuh's security device can also manage the Internet access from within the intranet based on the policy specified in the user profile.

vi. Appellant argues on page 13 that the Fuh's teaching and appellant's approach of the claimed Invention is different and argues that appellant's claimed approach provides for "determining whether or not to permit Internet access based on compliance with an access policy which specifies particular applications which are approved for Internet access". Appellant also argues that Fuh provides no teaching comparable to appellant's claim limitations of an access policy governing Internet access by client computers (see page 13).

In reply to [a. (vi)]: appellant argues that the teachings of Fuh referenced by the examiner indicate that Fuh's system decides whether or not to authenticate a user based on user login information and without examination of applications on the client computer.

As discussed above, the independent claims 1 and 45 does not explicitly teach and disclose "the process for determining whether or not to permit Internet access based on compliance with an access policy which **specifies particular applications which are approved for Internet access"** and the teaching of Fuh cited by the examiner was sufficient enough to reject the claims.

In conclusion, Fuh's firewall router does provide an access control mechanism for determining user access to a target server based on both user login information and a user profile, which includes specific rules and commands that specifies particular applications that are approved for Internet access (fig. 1, fig. 2 item #210, item #222, col. 2 L40-46 and col. 13 L44 to col. 14 L30: table 2 explicitly lists the examples of applications that are allowed access).

b. The examiner failed to establish a prima facie case of obviousness under section 103(a) because the references cited by the examiner failed to meet the conditions of establishing the prima facie case (page 14-15).

In reply to [b.]: Fuh discloses the process of hashing information such as source IP address, destination IP address, source port, destination port value and state information (col. 9 L55-63) and a user profile including applications (col. 14 L20-30), however Fuh does not disclose that the applications are specified by executable name and version number, application are specified by digital signatures, digital signatures are computed using a cryptographic hash and wherein said cryptographic hash comprises a selected one of Secure Hash Algorithm (SHA-1) and MD5 cryptographic hashes, however it would have been obvious to the one of ordinary skill in the art at the time the invention was made to incorporate these features because they are simply well known and obvious in the art and modify Fuh in order to specify the applications by their executable name and version numbers, specify applications by the digital signatures, wherein digital signatures are computed using cryptographic hash and wherein cryptographic hash comprises secure hash algorithm and MD5 cryptographic hashes. One of ordinary skilled in the art would have been motivated because it would have allowed a router to make a correct decision (block or permit) by comparing executable names and securely transfer the data to the destination by searching the profile efficiently.

Further the applicant traversal to rejection with respect to the subject matter above was inadequate. The applicant's traverse was considered inadequate because applicant failed to challenge the examiner's assertion of obviousness and/or well-known subject matter in response

to the first office action. As such, the common-knowledge (obviousness) or well-known subject matter is taken to be admitted prior art because applicant's traverse was inadequate (see MPEP 2144.03).

c. Logan's system does not teach anything analogous to appellant's claimed approach (see page 17).

In reply to [c.]: Logan's system is analogous to the appellant's claimed approach. Logan teaches the process of redirecting a request to a document (which is located at the server, col. 19 L63-67). Fuh teaches the process of checking for the compliance for the access (fig. 7A). That is, Fuh simply blocks the traffic (a request to access a resource on network) if the client is not in compliance whereas appellant's approach is that when a client is a non-compliant client, the client computer (i.e. client request for accessing the resource) is simply redirected to another server (appellant's sandbox server). Therefore there is a need in the Fuh's system for a process of redirecting the request or a client computer to another server simply by redirecting the client after the client is denied to access the Internet, which indeed is taught by Logan, i.e. redirecting a request to another server (Logan, col. 19 L63-67). Therefore, modifying Fuh in view of Logan by simply incorporating the process of redirecting a request to another server (Logan col. 19 L63-67) into Fuh's system would have resulted into the appellant's claimed approach of redirecting a request (a client computer as per appellant) that is not in compliance with the access policy (as disclosed by Fuh, see above) to a particular sandbox server (a server, as disclosed by Logan). As such, Logan does teach subject matter that is analogous to appellant's claimed approach.

d. Shrader does not cure the deficiencies of Fuh and Logan (see page 18).

In reply to [d.]: There are no deficiencies in Fuh and Logan as discussed above. And Shrader further teaches the subject matter disclosed in the dependent claims.

Further Shrader does disclose and teach the specific teaching of the appellant's claims 26 and 41 of permitting a client computer not in compliance with the access policy to elect to proceed with the access (interpreted as, the client is given another opportunity to login, i.e. elect to proceed with the Internet access, col. 4 L56-57). Shrader returns the error message and prompts the user and for ID and password again for the Internet access so that the process of authenticating and authorization can be performed again.

e. Durst does not cure deficiencies of Fuh and Durst (see page 18).

In reply to [e.]: There are no deficiencies in Fuh as discussed above.

f. The examiner's analysis appears to be simply conclusory hindsight, and not a thoughtful analysis of motivation provided by the cited references (see page 19).

In reply to [f.]: In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge

gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

ZARNI MAUNG
SUPERVISORY PATENT EXAMINER

Conferees:

Patrice Winder

PATRICE WINDER
PRIMARY EXAMINER

Zarni Maung